FINANSTILSYNET
THE FINANCIAL SUPERVISORY
AUTHORITY OF NORWAY

NORGES BANK

23.03.2021

Fra: Finanstilsynet og Norges Bank

Høringsnotat TIBER-NO

Innhold

1. Bakgrunn og formål

Tiltakende risiko for cyberkriminalitet og andre cyberangrep mot sentrale IKT-systemer er en utfordring for effektivitet og sikkerhet i finanssektoren i Norge.

For å redusere cybersikkerhetsrisikoen i finansiell sektor utarbeidet den europeiske sentralbanken (ECB) i 2018 rammeverket TIBER-EU («Threat Intelligence-Based Ethical Red-teaming»). TIBER-EU er retningslinjer for inntrengingstesting av finansielle institusjoners[1] evne til å oppdage, beskytte seg mot og reagere på avanserte cyberangrep. Formålet er å øke cybersikkerheten i finanssektoren og fremme finansiell stabilitet. Denne typen standardisert opplegg for trusselbasert testing er ikke etablert i finansiell sektor i Norge i dag.

TIBER-rammeverket er innført i mange europeiske land herunder Danmark, Sverige og Finland.

2. Prosess for å utvikle TIBER-NO

Norges Bank og Finanstilsynet har i fellesskap utarbeidet forslag til nasjonalt rammeverk for testing av cybersikkerhet, «TIBER-NO». De to institusjonene besluttet i første halvår 2020 at det skulle utarbeides et forslag til rammeverk for testing av cybersikkerheten i bank- og betalingssystemet i Norge[2] som skulle bygge på TIBER-EU. Beslutningen ble tatt på bakgrunn av positive tilbakemeldinger fra finansnæringen, jf. brev fra Finanstilsynet og Norges Bank 10. oktober 2019.

Næringen og relevante myndigheter er blitt informert om TIBER-NO mens arbeidet har pågått. Tilbakemeldinger og kommentarer er hensyntatt i forslaget som nå sendes på høring.

3. Gjeldende rammeverk for testing av cybersikkerhet i finansiell sektor i Norge

Det følger av sikkerhetsloven at virksomheter med skjermingsverdige informasjonssystemer kan be Nasjonal Sikkerhetsmyndighet (NSM) om å utføre inntrengningstester for å teste om etablerte kontrolltiltak er tilstrekkelige. Inntrengingstestene kan også utføres av tredjeparter som er godkjent av NSM.

Forskrift om bruk av informasjons- og kommunikasjonsteknologi (IKT) har bestemmelser om IKT-sikkerhet, og testing og forsvarlig drift for foretak i finansiell sektor. Disse følges opp gjennom Finanstilsynets tilsynsvirksomhet[3]. Det følger av formålsbestemmelsen i betalingssystemloven at interbanksystemer skal organiseres slik at hensynet til finansiell stabilitet blir ivaretatt. Betalingssystemloven stiller videre krav til at systemer for betalingstjenester innrettes og drives slik at hensynet til sikker og effektiv betaling og til rasjonell og samordnet utførelse av betalingstjenester ivaretas. Retningslinjer om IKT-sikkerhet og –risiko fra den europeiske banktilsynsmyndigheten[4] fra European Banking Authority (EBA) har bestemmelser om sikkerhetstesting.

[1] For the purposes of the TIBER-EU framework, «entities» («institusjoner») means: «payment systems, central securities depositories, central counterparty clearing houses, trade repositories, credit rating agencies, stock exchanges, securities settlement platforms, banks, payment institutions, insurance companies, asset management companies and any other service providers deemed critical for the functioning of the financial sector»

[2] https://www.finanstilsynet.no/nyhetsarkiv/nyheter/2020/rammeverk-for-testing-av-cybersikkerhet-tiber-no/

[3] Slike bestemmelser finnes i finanstilsynsloven og gjelder da for finansforetak

[4] Guideline for ICT Security and Risk Management

Norges Banks tilsyns- og overvåkingsarbeid med cybersikkerhet gjøres med grunnlag i internasjonale anbefalinger for finansiell infrastruktur[5]. Det følger av anbefalingene at foretak med ansvar for funksjoner i finansiell infrastruktur skal gjennomføre inntrengningstesting for å identifisere sårbarheter og redusere disse med tiltak.

4. Kommende EU-regulering av cybersikkerhetstesting

EU-kommisjonen har utarbeidet forslag til «Digital Operational Resilience Act for the financial sector» (DORA). DORA stiller krav til cybersikkerhetstesting og til andre områder relevante for digital robusthet. De europeiske tilsynsmyndighetene EBA[6], EIOPA[7] og ESMA[8] skal etter konsultering med ECB og hensyntatt eksisterende rammeverk utarbeide forslag til regulatoriske tekniske standarder for testrammeverk. Det antas at DORA vil være relevant for Norge og bli tatt inn i norsk rett som forskrift.

Bestemmelser i DORA som er særlig relevante for TIBER (artikkel 23 og 24) antas å tre i kraft først om tre til fem år.

5. Juridisk vurdering for TIBER-NO

Etableringen av TIBER-NO – som omfatter både rammeverk, metodikk og prosesser – vil ikke være i strid med noen norske eller EØS-relevante lover eller forskrifter.

Det er en forutsetning for denne konklusjonen at deltakelse i TIBER-NO er *frivillig* for alle aktører, og at Norges Bank har det formelle ansvaret for forvaltningen av rammeverket.

6. Organisering og ansvar

Finanstilsynet og Norges Bank samarbeider om implementering og bruk av TIBER-rammeverket i Norge og vil etablere de nødvendige fora for overordnet oppfølging, styring og involvering av næringsaktører og andre relevante myndigheter. Norges Bank organiserer og bemanner et «TIBER-NO Cyber Team» (TCT-NO) for å forvalte og operasjonalisere TIBER-NO, og har det formelle ansvaret for forvaltning av rammeverket.

Kostnadene for TIBER-Cyber-Team-NO (TCT-NO), som skal forvalte TIBER-NO og følge opp testingen, vil bli dekket av Norges Bank.

7. Kostnader for foretakene som testes

Foretakene som gjennomfører testing må selv dekke kostnader til interne ressurser og leverandører av etterretning og «Red Team»-testing.

TCT-NO vil bidra med blant annet å kvalitetssikre leveranser fra eksterne, herunder at leveransene tilfredsstiller kravene i TIBER-NO.

Erfaringen fra TIBER-testing i andre land viser at noen av foretakene som testes, bruker betydelig mer ressurser på hver TIBER-test enn på andre «Red Team»-tester. Kvaliteten og nytten av TIBER-tester oppleves imidlertid som større enn for andre «Red Team»-tester.

---

[5] Principles for Financial Market Infrastructures (PFMI) fra Committee on Payments and Market Infrastructures (CPMI) og the International Organization of Securities Commissions (IOSCO)
[6] European Banking Authority
[7] European Insurance and Occupational Pensions Authority
[8] European Securities and Markets Authority

Basert på erfaringsdata kan planlegging, gjennomføring og oppsummering av TIBER-tester strekke seg over flere måneder. Varigheten varierer med størrelsen på foretaket som testes, valgte testscenarier og hvilke kritiske funksjoner som testes.

Kostnadspådraget er vanligvis størst ved selve testgjennomføringen og mindre ved planlegging, etterretning og oppsummering/rapportering. Testingen vil normalt være oppad begrenset til et bestemt antall uker, fastsatt i kontrakt mellom foretaket som testes og «Red Team»-testleverandør. Det gir en øvre grense for kostnadene og gjør det enklere for foretakene som gjennomfører testing å ha kontroll.

8. Foreslåtte valg for TIBER-NO

TIBER-EU gir valgfrihet på noen områder. Nedenfor følger forslag til valg for TIBER-NO på disse områdene, med begrunnelse.

Generelle prinsipper

Formål

Det følger av TIBER-EU at:

- «The jurisdiction adopts the TIBER-framework as a supervisory or oversight tool, as a catalyst, or for the purposes of financial stability».

I Danmark, Sverige og Finland er TIBER innført for å fremme finansiell stabilitet. Åpenhet om testresultater og deling av erfaringer mellom deltakerne som testes, er vektlagt. Slik åpenhet kan stå i en viss motsats til direkte innsyn fra tilsyn og overvåking. For sterk kopling til tilsyn og overvåking i forbindelse med selve testgjennomføringen kan medføre at færre foretak velger å delta i TIBER-NO.

Erfaringene fra TIBER-EU er at foretak som testes etter TIBER ikke ønsker direkte innsyn fra tilsynsmyndigheter. Ved grensekryssende tester av internasjonale foretak kan det være viktig for foretakene som testes, at TIBER-rammeverket ikke er et tilsynsverktøy i andre land. Innspill fra bransjen[9] indikerer at ønsket om en viss avstand til tilsynsmyndigheter, også gjelder i Norge.

På bakgrunn av ovenstående foreslås følgende formål:

> **«Målsettingen for TIBER-NO er å bidra til finansiell stabilitet gjennom økt motstandsdyktighet mot cyberangrep for kritiske funksjoner i det norske finansielle systemet. TIBER-NO er ikke ment som et verktøy for tilsyn og overvåking av foretak og enkeltsystemer.»**

Frivillig eller obligatorisk deltakelse

Det følger av TIBER-EU at:

- «The jurisdiction determines which entities should undertake a test – either on a voluntary or mandatory basis».

TIBER innebærer omfattende og avansert testing som kan være dyrt og ressurskrevende for foretakene som testes. I alle de tre nordiske landene der TIBER er innført,[10] er det valgt å la deltakelse være frivillig. Bransjen i Norge har så langt gitt uttrykk for at det er ønskelig med harmonisering på tvers av de nordiske land. Det taler for frivillig deltakelse også i Norge. Den

[9] Spørreundersøkelsen 2019 og informasjonsmøter 28. januar, 19. november og 18. desember 2020
[10] Danmark, Sverige og Finland

juridiske vurderingen gjennomført av Norges Bank i forbindelse med TIBER-NO, forutsetter at deltakelse er frivillig for at Norges Bank skal kunne ta på seg forvaltningsansvaret for rammeverket.

Frivillig deltakelse i TIBER-NO kan gi en risiko for at sentrale aktører velger å ikke delta slik at målsettingen om å bidra til finansiell stabilitet ikke nås. For å oppnå målsettingen for TIBER-NO ser Finanstilsynet og Norges Bank det som avgjørende at sentrale aktører deltar.

Norges Bank og Finanstilsynet vil invitere/oppfordre foretak og systemeiere som er sentrale for finansiell stabilitet til å delta i og teste etter TIBER-NO, med utgangspunkt i hvilke funksjoner som har vesentlig betydning for finansiell stabilitet. Et viktig suksesskriterium for TIBER-NO er at funksjoner som er sentrale for finansiell stabilitet, blir testet.

På bakgrunn av ovenstående foreslås det at det er frivillig å delta i TIBER-NO.

Målgruppe

Det følger av TIBER-EU at:

- «The jurisdiction determines which entities should undertake a test»
- «Authorities should look to include entities which are important to the financial stability of the jurisdiction because of the critical functions (CFs) they perform»
- «The TIBER-EU framework can be applied to all types and sizes of entities».

For at testingen skal kunne bidra til økt motstandsdyktighet mot cyberangrep og dermed finansiell stabilitet, må en viss andel av «kritiske funksjoner» i finansiell sektor testes[11]. Det er derfor viktig å legge til rette for at TIBER-testingen inkluderer sentrale IKT-leverandører og datasentre. Mange norske banker samarbeider i allianser og har derfor de samme leverandørene.

Det er ønskelig at flest mulig foretak med ansvar for kritiske funksjoner herunder kritiske funksjoner i betalingssystemet, deltar i og tester etter TIBER-NO. TIBER-NO bør legge til rette for at norske filialer i internasjonale og nordiske konsern velger å delta, også dersom deres virksomhet i Norge ikke inkluderer kritiske funksjoner for finansiell stabilitet.

Testing av foretak som ikke har ansvar for kritiske funksjoner, kan bidra til å styrke finansiell stabilitet. Eksempelvis kan testing av ikke-kritiske funksjoner avdekke sårbarheter hos en leverandør som også benyttes av et foretak med ansvar for kritiske funksjoner. Dersom disse sårbarhetene reduseres, vil det kunne styrke sikkerheten også for foretaket med ansvar for kritiske funksjoner.

På bakgrunn av ovenstående foreslås følgende formulering:
«TIBER-NO er ment for foretak i finansiell sektor som har funksjoner som er kritiske for det norske finansielle systemet. For TIBER-NO er det likevel valgt at ikke-kritiske funksjoner også kan inkluderes i tester. Videre er det åpnet for at foretak i finansiell sektor som ikke har kritiske funksjoner kan delta i TIBER-NO og gjennomføre TIBER-tester».

Testing av kritiske funksjoner vil bli prioritert foran ikke-kritiske dersom det oppstår perioder der TCT-NO har kapasitetsbegrensninger.

[11] Det omfatter, men er ikke begrenset til, grunnleggende nasjonale funksjoner (GNF) slik det følger av Sikkerhetsloven. Merk at også DSB har publisert vurderinger av samfunnets kritiske funksjoner (KIKS).

Testprosessen

Generisk trusselrapport

Det følger av TIBER-EU at det er valgfritt hvorvidt en generisk trusselrapport (Generic Threat Landscape Report - GTL) skal utarbeides og oppdateres for hvert land som innfører TIBER. Denne GTL-rapporten utgjør, dersom den er tilgjengelig, et viktig grunnlag for den målrettede trusselrapporten som skal utarbeides for hver enkelt TIBER-test.

NFCERT utarbeider en felles nordisk GTL-rapport. Med nasjonale vedlegg som inneholder informasjon om finansiell infrastruktur i hvert land, møter rapporten kravene TIBER-EU stiller til GTL-rapporter. Rapporten benyttes som GTL-rapport for TIBER i Danmark og Finland.

Bruk av samme trusselrapport på tvers av Norden kan bidra til at nordiske TIBER-tester gjennomføres på samme grunnlag, og legger til rette for godt nordisk samarbeid. Videre vil en slik felles rapport være kostnadsreduserende og tidsbesparende.

På bakgrunn av ovenstående foreslås det at GTL-rapport er obligatorisk for TIBER-NO og at GTL-rapporten fra NFCERT med vedlegg om norsk finansiell infrastruktur benyttes.

Involvering av nasjonal trusseletterretning og sikkerhetstjenester

Det er etter TIBER-EU valgfritt om det skal stilles krav til at nasjonale etterretningsorgan, nasjonalt cybersikkerhetssenter eller politiets ansvarlige enheter på fagområdet inkluderes i testing eller andre deler av TIBER-prosessen. For TIBER-NO kan det være nyttig å etablere en knytning til denne typen organer, både for hver enkelt test og mer generelt.

NFCERT har ansvar for å utarbeide den nordiske GTL-rapporten, og NSM er involvert i arbeidet. NFCERT har videre en rolle i å støtte foretak i finanssektoren som utsettes for cyberangrep. NFCERT vil langt på vei ha denne rollen også i forbindelse med TIBER-testing[12], fordi foretak som testes etter TIBER vil oppleve testingen som reelle angrep[13].

Avklaringer med sikte på obligatorisk involvering av andre myndigheter enn Norges Bank og Finanstilsynet kan forsinke etableringen av TIBER-NO. Det vil også kunne gjøre TIBER-NO mindre fleksibelt.

Obligatorisk involvering kan imidlertid øke kvaliteten av testing, for eksempel ved at kunnskapen som nasjonal etterretning besitter mer aktivt tas i bruk ved planlegging av testing.

På bakgrunn av ovenstående foreslås det at involvering av nasjonale etterretnings- og sikkerhetstjenester er frivillig ved testing etter TIBER-NO, både for TCT-NO og foretakene som gjennomfører testing.

Involvering av andre myndigheter i testing

Det følger av TIBER-EU at det er valgfritt om andre myndigheter skal involveres i oppstartsmøte for hver enkelt test. Eksempler på myndigheter som kan være relevante for slike møter er NKOM[14] og NSM[15].

[12] Forutsetter at foretaket er NFCERT-medlem
[13] Med unntak for «White Team» i foretaket, som kjenner til testen
[14] Nasjonal kommunikasjonsmyndighet
[15] Nasjonal sikkerhetsmyndighet

TCT-NO deltar i oppstartsmøte med foretakene for TIBER-NO-tester, er ansvarlig for kommunikasjon med andre relevante myndigheter og kan be om at myndighetsorganer blir invitert til oppstartsmøter dersom det kan bidra til å øke verdien på testingen eller er nyttig på andre måter.

Obligatorisk deltakelse av myndigheter kan på den annen side medføre at TIBER-testingen oppleves som mer tungrodd for deltakende foretak.

På bakgrunn av ovenstående foreslås det at TCT-NO og foretaket som testes kan involvere andre myndigheter i testingen, men at dette ikke er obligatorisk etter TIBER-NO.

Oppdatering av etterretning

Det følger av TIBER-EU at det er valgfritt om leverandør av trusseletterretning for en enkelt test fortsetter engasjementet mens testingen pågår og leverer oppdatert etterretning når det er relevant. For TIBER-NO er det i tråd med tilbakemeldinger fra bransjen (i møtet 19. november 2020) vektlagt å holde kostnadene på et rimelig nivå. Obligatorisk utvidelse av engasjementet for leverandøren av trusseletterretning er kostnadsdrivende. Høyere kostnader kan medføre at færre virksomheter velger å delta. Merverdien for foretaket av oppdaterte etterretningsdata gjennom testperioden antas å være relativt lav i mange tilfeller. At dette ikke gjøres obligatorisk for TIBER-NO er ikke til hinder for at virksomhetene som testes kan velge å gjøre det. Hvert enkelt foretak har incentiver til oppdatering av etterretning dersom det forventes å være lønnsomt.

Det foreslås at oppdatering av etterretning gjennom testperioden er frivillig etter TIBER-NO.

Bruk av fysiske gjenstander i testingen

Det følger av TIBER-EU at:

- «The jurisdiction, in its implementation of the TIBER framework, allows physical red teaming in the scope of the methodology for the TIBER test (e.g. planting a device at the entity), provided all necessary precautions are taken».

Hvert enkelt land kan velge å tillate bruk av ulike fysiske gjenstander som minnepinner, komponenter knyttet til trådløse nett mv. som del av testing. Hvis en slik metode tillates for TIBER-NO og anvendes for konkret TIBER-testing av et foretak, vektlegger TIBER-EU at formelt samtykke fra foretaket som testes skal være på plass og at ingen etiske eller juridiske grenser skal krysses.

For scenarioer hvor fysiske virkemidler er en realistisk angrepsmetode (angrepsvektor), f.eks. «planting» av USB, har «White Team» i det testede foretaket ansvar for å vurdere om slik testing skal gjennomføres med tanke på kostnader, tidsbruk og risiko.

TIBER-DK, -SE og- FI har åpnet for bruk av fysiske gjenstander som del av testingen.

På bakgrunn av ovenstående foreslås det at bruk av fysiske gjenstander (minnepinner mv.) tillates etter TIBER-NO. Foretakets «White Team» må sørge for at det gjøres en grundig risikovurdering forut for hver test. Eventuelle tiltak for å redusere testrisiko må gjennomføres før testing igangsettes.

Utvide enkelttester til å inkludere funksjoner som ikke er kritiske

Det følger av TIBER-EU at nasjonale rammeverk kan åpne for at enkelttester - i foretak med ansvar for mer overordnede kritiske funksjoner - kan inkludere testing av funksjoner som ikke er kritiske:

- «The entity expands the scope of the test beyond the CFs and includes other functions and processes».

Dersom TIBER-NO åpner for testing av ikke-kritiske funksjoner, vil det blir mer fleksibelt for foretakene som tester å planlegge og gjennomføre TIBER-tester. Bransjen har gitt innspill om at TIBER-NO ikke må bli for stivbent.

På bakgrunn av ovenstående foreslås det at testing etter TIBER-NO kan inkludere ikke-kritiske funksjoner hos foretaket som testes.

Scenarier som ikke er avtalt på forhånd

Scenario X innebærer at leverandør av testing («Red Team Provider») kan teste etter scenarier testleverandør selv utformer etter at testen har startet. Slik kan «Red Team Provider» foreslå nye veier til målet basert på erfaringer tilegnet i løpet av angrepsfasen (testingen). Scenario X må etter TIBER-EU godkjennes av foretaket ved leder for «White Team» og TCT-NO i hvert enkelt tilfelle.

Målet med Scenario X er å gjøre testingen mer realistisk og mer lik avanserte angrep. Dersom TIBER-NO åpner for Scenario X, kan leder for «White Team» tillate Scenario X i en konkret TIBER-NO test der det passer til trusselaktørens måte å operere på (modus operandi).

Scenario X gir «Red Team Provider» mulighet til å foreslå innovative teknikker og taktikker for å oppnå målet. Det kan øke kvaliteten på testen og nytteverdien for den testede virksomheten. Scenario X kan gi mer reell testing og bidra til å redusere cyberrisikoen for foretaket som testes. På den annen side kan Scenario X medføre økt risiko under testingen.

Nederland viser til gode erfaringer med Scenario X ved testing etter TIBER-NL. TIBER-DK tillater bruk av Scenario X. TIBER-SE og -FI nevner ikke Scenario X i sine TIBER-veiledninger.

Innspill fra norsk finansbransje har så langt pekt i retning av at det er ønskelig å beholde fleksibilitet. Scenario X gir mer fleksibilitet i testing gjennom løpende tilpasning av test-scenarier basert på hvordan foretaket responderer på testingen. Justering av planlagte test-scenarioer mens testen pågår kan være formålstjenlig dersom noe av hensikten er å teste hvordan «Blue Team» responderer. Eksempelvis kan et scenario endres og gjentas med mer støy dersom «Blue Team» ikke oppdager test-angrepet.

På bakgrunn av ovenstående foreslås det at TIBER-NO tillater Scenario X-testing. «White Team» i foretaket som testes har ansvar for å godkjenne Scenario X-testing.

«Purple Teaming»

Det følger av TIBER-EU at:

- «A purple teaming element is added in which the «Blue Team» and the «Red Team» provider can work together to see which other steps could have been taken by the «Red Team» provider and how the «Blue Team» could have responded to those steps»

Oppsummeringsmøter etter TIBER-testing er obligatorisk. Det vil være ulike deltakere i de ulike møtene, men alle leverandører og interne «team» i foretaket deltar i minst ett av oppsummeringsmøtene. Etter TIBER-EU er det valgfritt om det skal gjennomføres et felles møte for «Blue Team» og «Red Team» dvs. såkalt «Purple Teaming». Erfaringer fra andre land viser at «Purple Teaming» gir stor gevinst for foretaket som ble testet, og det oppfordres til dette. For TIBER-NO er det imidlertid vektlagt å beholde fleksibilitet.

På bakgrunn av ovenstående foreslås det at «Purple Teaming» er valgfritt etter TIBER-NO.